ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR COMPUTING DIGITAL CERTIFICATE TRUST PATHS USING TRANSITIVE CLOSURES

A method, system, apparatus, and computer program product are presented for managing digital certificates. When entities need to engage in a secure transaction or open a secure communication link, they may exchange digital certificates in order to provide a public key or reference information to a public key for the opposing entity, thereby requiring validation of a received certificate. Rather than construct a trust path for each validation event, hierarchical certifications and peer-to-peer cross-certifications among a set of certificate authorities are represented by a set of trust relations, and trust path information is generated using a transitive closure computation and an "all pairs shortest paths" computation over the set of trust relations and then incrementally updated as the set of trust relations changes. Computations related to trust paths can be delegated to a central agent in a trust web.